UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/672,342	09/26/2003	Hiroaki Etoh	JP920020149US1	9697

54856 7590 05/25/2007

LOUIS PAUL HERZBERG
3 CLOVERDALE LANE
MONSEY, NY 10952

EXAMINER	
LASHLEY, LAUREL L	
ART UNIT	**PAPER NUMBER**
2132	
MAIL DATE	**DELIVERY MODE**
05/25/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/672,342	ETOH ET AL.	
	Examiner	Art Unit	
	Laurel Lashley	2132	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *12 March 2007*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-20* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-20* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

Response to Amendment

1. Applicant's amendments with respect to claims 1, 4, 7, 10 and new claims 19 and 20 filed 03/21/07 have been accepted. Therefore claims 1 – 20 are pending. The amendments however have introduced some claims objections.

Claim Objections

2. Claim 19 is objected to because of the following informalities:

- Recitation of numeral 2 after introducing claim 19 as a new claim.
- Unnecessary usage of an open parenthesis at the end of the claim.

Appropriate correction is required.

Response to Arguments

3. Applicant's arguments filed 03/21/2007 have been fully considered but they are not persuasive. It is Applicant's primary assertions that Porras does not disclose monitoring in real time and does not use packet streams. The Examiner respectfully disagrees. Porras discloses real-time analysis of network packets as performed by service monitors (see column 3, lines 51 – 53). This analysis results in the statistical profiling of events streams (see column 5, lines 46 – 50). Furthermore, in response to applicant's argument that Porras is based on statistics, a recitation of the intended use of the claimed invention must result in a structural difference between the claimed invention and the prior art in order to patentably distinguish the claimed invention from the prior art. If the prior art structure is capable of performing the intended use, then it meets the claim.

In particular, it is Applicant's argument that claim 1, Porras does not allude to "a communications sensor for receiving and monitoring in real time communications packets flowing at arbitrary points on a network, said communications being any of communications

conducted via a host and communications conducted directly" or does not anticipate "calculating formal similarity between two packet streams composed of communications packets entering the sensor upon arrival of the communications packets, and said sensor employing said formal similarity in detecting an intrusion." Again Porras discloses dynamic deployment of network monitors that are responsible for real time surveillance of a network (see column 3, lines 41 – 63). The short and long term statistical profiles aid in the generation of a statistical score that represents the similarities between the identified network packet streams that were subjected to network surveillance. (see column 5, lines 46 – 50; column 6, lines 20 - 23)

As for claim 2, it is Applicant's assertion that Porras does not anticipate Claim 2's limitation in regard to "two packet streams by graphs depicting amounts of data in communications packets in respective packet streams with respect to elapsed time, and calculates similarity between the two packet streams." Porras teaches surveillance of event streams which are derived of network packet observation and collection (see column 1, lines 51 - 53). Moreover, the short and long term profiles of Porras are equivalent to the graphs depicting data communications since the profiles consist of data communication information (see column 1, lines 53 – 61; column 2, lines 49 - 60). The functionality and purpose of the profiles are parallel to those of the graphs as taught in Applicant's claimed invention.

Applicant has presents similar arguments to those addressed in respect to claims 1 and 2 and therefore the rejections of these claims are maintained for similar reasons.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in a patent granted on an application for patent by another filed in the United States before the invention thereof by the applicant for patent, or on an international application

> by another who has fulfilled the requirements of paragraphs (1), (2), and (4) of section 371(c) of this title before the invention thereof by the applicant for patent.

The changes made to 35 U.S.C. 102(e) by the American Inventors Protection Act of 1999 (AIPA) and the Intellectual Property and High Technology Technical Amendments Act of 2002 do not apply when the reference is a U.S. patent resulting directly or indirectly from an international application filed before November 29, 2000. Therefore, the prior art date of the reference is determined under 35 U.S.C. 102(e) prior to the amendment by the AIPA (pre-AIPA 35 U.S.C. 102(e)).

4. Claims 1 – 20 are rejected under 35 U.S.C. 102(e) as being anticipated by Porras et al. in US Patent No. 6711615 (hereinafter US '615).

5. As for claim 1, US '615 discloses:

A communications monitoring system comprising:

a communications sensor for receiving and monitoring in real time communications packets flowing at arbitrary points on a network, said communications being any of communications conducted via a host and communications conducted directly; and

a similarity calculator for calculating formal similarity between two packet streams composed of communications packets entering the sensor upon arrival of the communications packets, and said sensor employing said formal similarity in detecting an intrusion. (see column 1, line 52, 56 – 61; column 5, lines 46 – 50, 58 – 61; Abstract)

For claim 2, US '615 discloses:

The communications monitoring system according to claim 1, wherein the similarity calculator represents the two packet streams by graphs depicting amounts of data in communications packets in respective packet streams with respect to elapsed time, and calculates similarity between the two packet streams based on size of regions enclosed by the two graphs when the

graphs of the packet streams are moved close to each other without intersecting each other. (see column 6, lines 7 – 15)

For claim 3, US '615 discloses:

The communications monitoring system according to claim 1, wherein the communications sensor sends out a predetermined alert according to a similarity value calculated by the similarity calculator. (see column 4, lines 64 – 66; column 8, lines 23 – 39, 57 – column 9, lines 1 – 5)

As for claim 4, US '615 discloses:

A communications monitoring system comprising: a packet input means for receiving communications packets flowing at arbitrary points on a network, said communications being any of communications conducted via a host and communications conducted directly; and matching means for performing real-time matching between two packet streams composed of communications packets received by the packet input means and employing said real-time matching in detecting an intrusion. (see column 1, line 52, 56 – 61; column 5, lines 46 – 50, 58 – 61; Abstract)

For claim 5, US '615 discloses:

The communications monitoring system according to claim 4, wherein the matching means determines formal similarity between the two packet streams based on a time lag between each corresponding pair of communications packets in the two packet streams. (see column 6, lines 7 – 15)

For claim 6, US '615 discloses:

The communications monitoring system according to claim 5, further comprising alerting means for sending out a predetermined alert according to the formal similarity between the two packet

streams determined by the matching means. (see column 4, lines 64 – 66; column 8, lines 23 – 39, 57 – column 9, lines 1 – 5)

As for claim 7, US '615 discloses:

A communications monitoring method for monitoring data communications using a computer, comprising the steps of: acquiring in real time communications packets in sequence from arbitrary points on a network and storing them in predetermined storage means together with information about a packet stream to which the communications packets belong, said communications being any of communications conducted via a host and communications conducted directly; on reception of a predetermined communication packet, taking another communications packet received within a predetermined time before acquiring a predetermined communications packet, out of the storage means; determining formal similarity between the first packet stream which contains up to the acquired communications packet and a second packet stream to which the communications packet taken out of the storage means belong; and sending out a predetermined alert according to the determined similarity. (see column 1, line 52, 56 – 61; column 5, lines 46 – 50, 58 – 61; Abstract)

For claim 8, US '615 teaches:

The communications monitoring method according to claim 7, wherein in the step of determining the formal similarity of packet streams, the formal similarity between the two packet streams is determined based on a time lag between each corresponding pair of communications packets in the two packet streams. (see column 6, lines 7 – 15)

For claim 9, US '615 teaches:

The communications monitoring method according to claim 7, further comprising a step of discarding information used in determining the similarity of second packet streams except the

second packet stream determined to be most similar to the first packet stream. (see column 6, lines 7 – 15; column 8, lines 23 – 39, 57 – column 9, lines 1 – 5)

As for claim 10, US '615 teaches:

An information processing method comprising comparing two packet streams flowing in real time on a network, the step of comparing comprising the steps of: acquiring communications packets in sequence from arbitrary points on a network and storing them in predetermined storage means together with information about a packet stream to which the communications packets belong, said communications packets being in any of communications conducted via a host and communications conducted directly; on reception of a predetermined communication packet, taking another communications packet received within a predetermined time before acquiring a predetermined communications packet, out of the storage means; and performing matching between the first packet stream which contains up to the acquired communications packet and a second packet stream to which the communications packet taken out of the storage means belong. (see column 1, line 52, 56 – 61; column 5, lines 46 – 50, 58 – 61; Abstract)

For claim 11, US '615 teaches:

The information processing method according to claim 10, wherein in the step of performing matching between the packet streams, the first and second packet streams are represented by graphs which depict increments of sequence numbers of communications packets in respective packet streams with respect to elapsed time and the similarity between the two packet streams is calculated based on size of regions enclosed by the two graphs when the graphs of the packet streams are moved close to each other without intersecting each other. (see column 6, lines 7 – 15)

For claim 12, US '615 teaches:

The information processing method according to claim 11, wherein in the step of calculating the similarity between the packet streams, information used in determining the similarity is discarded according to time-axis lengths of the regions enclosed by the two graphs. (see column 6, lines 7 – 15; column 8, lines 23 – 39, 57 – column 9, lines 1 – 5)

For claim 13, US '615 teaches:

An article of manufacture comprising a computer usable medium having computer readable program code means embodied therein for causing communications monitoring, the computer readable program code means in said article of manufacture comprising computer readable program code means for causing a computer to effect the steps of claim 7. (see Figure 6)

For claim 14, US '615 teaches:

A program storage device readable by machine, tangibly embodying a program of instructions executable by the machine to perform method steps for communications monitoring, said method steps comprising the steps of claim 7. (see Figure 6)

For claim 15, US '615 teaches:

An article of manufacture comprising a computer usable medium having computer readable program code means embodied therein for causing information processing, the computer readable program code means in said article of manufacture comprising computer readable program code means for causing a computer to effect the steps of claim 10. (see Figure 6)

For claim 16, US '615 teaches:

A program storage device readable by machine, tangibly embodying a program of instructions executable by the machine to perform method steps for information processing, said method steps comprising the steps of claim 10. (see Figure 6)

For claim 17, US '615 teaches:

A computer program product comprising a computer usable medium having computer readable program code means embodied therein for causing communications monitoring, the computer readable program code means in said computer program product comprising computer readable program code means for causing a computer to effect the functions of claim 1. (see column 2, lines 32 – 36; Figure 6)

For claim 18, US '615 teaches:

A computer program product comprising a computer usable medium having computer readable program code means embodied therein for causing communications monitoring, the computer readable program code means in said computer program product comprising computer readable program code means for causing a computer to effect the functions of claim 4. (see column 2, lines 32 – 36; Figure 6)

For claim 19, US '615 teaches:

The communications monitoring system according to Claim 1, wherein the similarity calculator represents the two packet streams by graphs depicting amounts of data in communications packets in respective packet streams with respect to elapsed time, and calculates similarity between the two packet streams based on size of regions enclosed by the two graphs when the graphs of the packet streams are moved close to each other without intersecting each other, (see column 6, lines 7 – 15) and

wherein the communications sensor sends out a predetermined alert according to a similarity value calculated by the similarity calculator.((see column 4, lines 64 – 66; column 8, lines 23 – 39, 57 – column 9, lines 1 – 5)

For claim 20, US '615 teaches:

The information processing method according to Claim 10, wherein in the step of performing

matching between the packet streams, the first and second packet streams are represented by graphs which depict increments of sequence numbers of communications packets in respective packet streams with respect to elapsed time and the similarity between the two packet streams is calculated based on size of regions enclosed by the two graphs when the graphs of the packet streams are moved close to each other without intersecting each other, (see column 6, lines 7 – 15) and

wherein in the step of calculating the similarity between the packet streams, information used in determining the similarity is discarded according to time-axis lengths of the regions enclosed by the two graphs (see column 6, lines 7 – 15; column 8, lines 23 – 39, 57 – column 9, lines 1 – 5).

Conclusion

6. **THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

7. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Laurel Lashley whose telephone number is 571-272-0693. The examiner can normally be reached on Monday - Thursday, alt Fridays btw 7:30 am & 5 pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron, Jr. can be reached on 571-272-3799. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Laurel Lashley
Examiner
Art Unit 2132

LLL
21 May 2007

GILBERTO BARRÓN JR
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100